

Claims:

1. An ad-hoc radio communication verification system,
comprising :

means for sending data for verification data generation
5 from one data send/receive device to the other send/receive
device, wherein the two send/receive devices are mutually
connected by an ad-hoc radio connection;

in the one data send/receive device, means for
generating verification data from the sent data for
10 verification data generation based on a first generation
algorithm and outputting the generated verification data to
its own verification data output section;

in the other data send/receive device, means for
generating verification data from the received data for
15 verification data generation based on the first generation
algorithm and outputting the generated verification data to
its own verification data output section; and

means for determining whether the verification data at
the verification data output sections of both the data
20 send/receive devices matches mutually.

2. The ad-hoc radio communication verification system
according to claim 1, wherein the verification data is
visual or auditory verification data.

3. The ad-hoc radio communication verification system
25 according to claim 1, wherein the verification data is
output at the verification data output section both in the

visual form and auditory form.

4. The ad-hoc radio communication verification system according to claim 1, further comprising:

means for defining a function as an operator, a numeric
5 on which the operator operates as an input of the operator,
and an operation result of the operator as an output of the operator;

means for establishing a serial sequence of operators
that are composed of one or more of operators arranged in
10 series, wherein the operators relate to the same or
different one-way functions; and

means for letting an input to the serial sequence of
operators be the data for verification data generation and
an output from the serial sequence of operators or a
15 corresponding value be the verification data.

5. The ad-hoc radio communication verification system
according to claim 1, wherein the first generation algorithm
generates a plurality of verification data, wherein for each
verification data, it is determined whether the verification
20 data at the verification data output sections of both the
data send/receive devices match mutually.

6. The ad-hoc radio communication verification system
according to claim 5, further comprising:

means for defining a function as an operator, a numeric
25 on which the operator operates as an input of the operator,
and an operation result of the operator as an output of the

operator;

means for establishing a serial sequence of operators that are composed of two or more of operators arranged in series, wherein the operators relate to the same or
5 different one-way functions;

means for letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or
10 corresponding values be the verification data respectively; and

means for determining for each verification data whether the verification data match mutually at the verification data output sections of both the data
15 send/receive devices.

7. The ad-hoc radio communication verification system according to claim 5, further comprising:

means for defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the
20 operator;

means for establishing a plurality of operators that relate to mutually different one-way functions;

means for letting the data for verification data generation be a common input to each operator and an output of each operator or a corresponding value be the
25 verification data respectively; and

means for determining for each verification data

whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

8. The ad-hoc radio communication verification system according to claim 1, wherein the data for verification data generation is a public key of either data send/receive device.

9. An ad-hoc radio communication data send/receive system utilizing the ad-hoc radio communication verification system according to claim 8, comprising a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the ad-hoc radio communication verification system verifies that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key K_p is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key K_c based on a second generation algorithm, while the personal computer of the one user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data in cipher according

to the symmetric key Kc.

10. An ad-hoc radio communication data send/receive system
utilizing the ad-hoc radio communication verification system
according to claim 8, comprising a portable terminal having
5 a radio communication function and a personal computer
having a radio communication function that are owned by each
user, wherein the portable terminal and personal computer of
each user are connected by a secure communication path; when
the ad-hoc radio communication verification system verifies
10 that a public key Kp of one user is transmitted from the
portable terminal of the one user to the portable terminal
of the other user without being tampered with, the portable
terminal of the other user generates a symmetric key Kc
based on a second generation algorithm, while the portable
15 terminal of the one user generates the symmetric key Kc
based on the second generation algorithm from information
transmitted from the portable terminal of the other user in
cipher according to the public key, then the symmetric key
Kc is transmitted from the portable terminal to the personal
20 computer of each user; and thereafter both the personal
computers send and receive data in cipher according to the
symmetric key Kc.

11. An ad-hoc radio communication data send/receive system,
comprising a portable terminal having a radio communication
25 function and a personal computer having a radio
communication function that are owned by each user, wherein
the portable terminal and personal computer of each user are

connected by a secure communication path; when it is
verified that a public key K_p of one user is transmitted
from the portable terminal of the one user to the portable
terminal of the other user without being tampered with, the
5 public key K_p is transmitted from the portable terminal to
the personal computer of each user, then the personal
computer of the other user generates a symmetric key K_c
based on a second generation algorithm, while the personal
computer of the one user generates the symmetric key K_c
10 based on the second generation algorithm from information
transmitted from the personal computer of the other user in
cipher according to the public key; and thereafter both the
personal computers send and receive data in cipher according
to the symmetric key K_c .

12. An ad-hoc radio communication data send/receive system,
comprising a portable terminal having a radio communication
function and a personal computer having a radio
communication function that are owned by each user, wherein
the portable terminal and personal computer of each user are
15 connected by a secure communication path; when it is
verified that a public key K_p of one user is transmitted
from the portable terminal of the one user to the portable
terminal of the other user without being tampered with, the
portable terminal of the other user generates a symmetric
20 key K_c based on a second generation algorithm, while the
portable terminal of the one user generates the symmetric
key K_c based on the second generation algorithm from
information transmitted from the portable terminal of the
25

other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; thereafter both the personal computers send and receive data in cipher according to the symmetric key Kc.

13. A method for verifying an ad-hoc radio communication, comprising the steps of:

sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, generating verification data from the sent data for verification data generation based on a first generation algorithm and outputting the generated verification data to its own verification data output section;

in the other data send/receive device, generating verification data from the received data for verification data generation based on the first generation algorithm and outputting the generated verification data to its own verification data output section; and

determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.

14. The method according to claim 13, wherein the verification data is visual or auditory verification data.

15. The method according to claim 13, wherein the verification data is output at the verification data output section both in the visual form and auditory form.

16. The method according to claim 13, further comprising the steps of:

defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator;

establishing a serial sequence of operators that are composed of one or more of operators arranged in series, wherein the operators relate to the same or different one-way functions;

letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

17. The method according to claim 13, wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.

18. The method according to claim 17, further comprising the steps of:

defining a function as an operator, a numeric on which

the operator operates as an input of the operator, and an operation result of the operator as an output of the operator;

establishing a serial sequence of operators that are composed of two or more of operators arranged in series, wherein the operators relate to the same or different one-way functions;

letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively; and

determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

19. The method according to claim 17, further comprising the steps of:

defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator;

establishing a plurality of operators that relate to mutually different one-way functions;

letting the data for verification data generation be a common input to each operator and an output of each operator or a corresponding value be the verification data respectively; and

determining for each verification data whether the

verification data match mutually at the verification data
output sections of both the data send/receive devices.

20. The method according to claim 13, wherein the data for
verification data generation is a public key of either data
5 send/receive device.

21. The method for sending and receiving ad-hoc radio
communication data, utilizing the verification method
according to claim 20, comprising: a portable terminal
having a radio communication function and a personal
10 computer having a radio communication function that are
owned by each user, wherein the portable terminal and
personal computer of each user are connected by a secure
communication path; when the verification method verifies
that a public key K_p of one user is transmitted from the
15 portable terminal of the one user to the portable terminal
of the other user without being tampered with, the public
key K_p is transmitted from the portable terminal to the
personal computer of each user, then the personal computer
of the other user generates a symmetric key K_c based on a
20 second generation algorithm, while the personal computer of
the one user generates the symmetric key K_c based on the
second generation algorithm from information transmitted
from the personal computer of the other user in cipher
according to the public key; and thereafter both the
25 personal computers send and receive data in cipher according
to the symmetric key K_c .

22. The method for sending and receiving ad-hoc radio communication data, utilizing the verification method according to claim 20, comprising: a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the verification method verifies that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the portable terminal of the other user generates a symmetric key K_c based on a second generation algorithm, while the portable terminal of the one user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key K_c is transmitted from the portable terminal to the personal computer of each user; and thereafter both the personal computers send and receive data in cipher according to the symmetric key K_c .

23. The method for sending and receiving ad-hoc radio communication data, comprising: a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key K_p of one user is transmitted

from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key K_p is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key K_c based on a second generation algorithm, while the personal computer of the one user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data in cipher according to the symmetric key K_c .

24. The method for sending and receiving ad-hoc radio communication data, comprising: a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the portable terminal of the other user generates a symmetric key K_c based on a second generation algorithm, while the portable terminal of the one user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key K_c is transmitted from the portable terminal

to the personal computer of each user; thereafter both the personal computers send and receive data in cipher according to the symmetric key Kc.

25. A recording medium recording a program for an ad-hoc radio communication verification system, wherein the verification system comprising:

means for sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, means for generating verification data from the sent data for verification data generation based on a first generation algorithm and outputting the generated verification data to its own verification data output section;

in the other data send/receive device, means for generating verification data from the received data for verification data generation based on the first generation algorithm and outputting the generated verification data to its own verification data output section; and

means for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.

26. The recording medium according to claim 25, wherein the verification data is visual or auditory verification data.

27. The recording medium according to claim 25, wherein the

verification data is output at the verification data output section both in the visual form and auditory form.

28. The recording medium according to claim 25, wherein the verification system further comprising:

5 means for defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator;

10 means for establishing a serial sequence of operators that are composed of one or more of operators arranged in series, wherein the operators relate to the same or different one-way functions; and

15 means for letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

20 29. The recording medium according to claim 25, wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.

25 30. A delivery system for delivering a program for an ad-hoc radio communication system, the verification system comprising:

means for sending data for verification data generation

from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, means for
5 generating verification data from the sent data for verification data generation based on a first generation algorithm and outputting the generated verification data to its own verification data output section;

10 in the other data send/receive device, means for generating verification data from the received data for verification data generation based on the first generation algorithm and outputting the generated verification data to its own verification data output section; and

15 means for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.

31. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer
20 readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the the funtions of claim 1.

32. 31. A computer program product comprising a computer usable medium having computer readable program code means

embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the the functions of claim 1.

5 33. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a
10 computer to effect the the functions of claim 9.

34. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product
15 comprising computer readable program code means for causing a computer to effect the the functions of claim 10.

35. A computer program product comprising a computer usable medium having computer readable program code means embodied

therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 11.

5 36. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a
10 computer to effect the functions of claim 30.

37. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture
15 comprising computer readable program code means for causing a computer to effect the steps of claim 13.

38. An article of manufacture comprising a computer usable medium having computer readable program code means embodied

therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 21.

5 39. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a
10 computer to effect the steps of claim 22.

40. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture
15 comprising computer readable program code means for causing a computer to effect the steps of claim 23.

41. An article of manufacture comprising a computer usable medium having computer readable program code means embodied

therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 24.

5 42. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a
10 computer to effect the steps of claim 24.

43. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture
15 comprising computer readable program code means for causing a computer to effect the steps of claim 25.